ABSTRACT

Inbound and outbound traffic on a computer system are intercepted and compared to determine if the presence of malicious code is indicated. Outbound traffic that is sufficiently similar to recently received inbound traffic is indicative of the presence of malicious code. In some embodiments, if the presence of malicious code is indicated, the user, as well as other individuals or systems, are notified of the detection. In some embodiments, if desired, protective actions are initiated to hinder or block the propagation of the malicious code from the host computer system to other computer systems, as well as to remove or inactivate the malicious code on the host computer system.